项目 3　网络协议与分析

【项目目标】

(1) 了解 OSI 参考模型和 TCP/IP 参考模型。
(2) 了解以太网的帧格式。
(3) 了解网络层协议和传输层协议。
(4) 了解三次握手机制。
(5) 掌握 ARP 欺骗攻击的原理和防范方法。
(6) 会使用 Sniffer 抓包软件。
(7) 了解端口镜像。

3.1　项 目 提 出

张先生在企业的网络中心工作,负责整个企业网络的管理和维护,作为网络管理员需要时刻了解企业网络流量情况,并对网络流量进行监控,以便及时发现并解决可能出现的网络问题。最近有多位企业员工反映,近期访问外网的速度时快时慢,甚至不能访问外网,请求网络中心给予解决。

3.2　项 目 分 析

从各位员工反映的上网情况来看,网速变慢是最近发生的事情,近期企业内部没有进行网络设备的调整,网络环境没有发生变化,网络应用也没有大的变化,这应该是网络中有异常流量造成的。

张先生经过调查发现,网络中存在以下网络故障现象。

(1) 某部门的所有计算机配置相同,且处于同一个网段,唯独某一台计算机无法上网,而且网络、网络接口等都正常,该计算机重新启动后网络恢复正常,过一段时间后,网络又瘫痪了。

(2) 网络中的计算机逐台掉线,最后导致全部计算机无法上网。

(3) 某计算机上网时突然掉线,一会儿又恢复了,但恢复后上网一直很慢,而且在与局域网内的其他计算机共享文件时速度也变慢。

(4) 网络中用户上不了网或者网速很慢。

张先生用网络监听工具 Sniffer Pro 来嗅探网络中的数据包,发现网络中存在大量的 ARP 数据包,而且计算机 ARP 缓存表中的网关 MAC 地址已被修改,导致网络变慢甚至无法上网,这就是典型的 ARP 欺骗攻击。

在计算机中利用"ARP -s 网关 IP 网关 MAC"命令静态设置正确的网关 MAC 地址,在网关(一般是路由器)中对局域网内的主机 IP 地址与其相应的 MAC 地址也进行静态绑定,上网恢复正常。

3.3　相关知识点

3.3.1　计算机网络体系结构

1. OSI 参考模型

在计算机网络诞生之初,每个计算机厂商都有一套自己的网络体系结构,之间互不相容。为此,国际标准化组织(ISO)在 1979 年建立了一个分委员会来专门研究一种用于开放系统互联的体系结构,即 OSI。"开放"这个词表示:只要遵循 OSI 标准,一个系统可以和位于世界上任何地方的,也遵循 OSI 标准的其他任何系统进行连接。这个分委员会提出了开放系统互联参考模型,即 OSI 参考模型(OSI/RM),它定义了异类系统互联的标准框架。OSI/RM 模型分为 7 层,从下往上分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层,如图 3-1 所示。

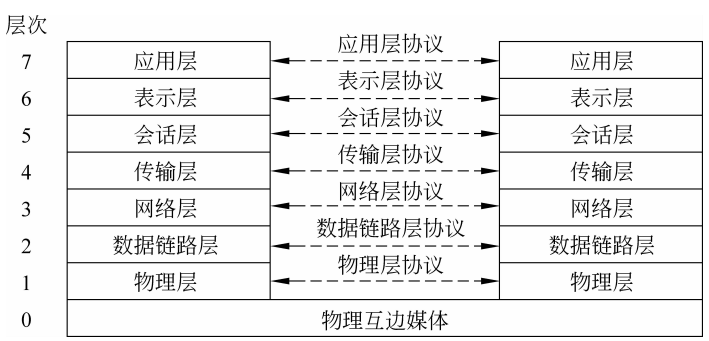

图 3-1　OSI/RM 模型

计算机网络体系结构是计算机网络层次模型和各层协议的集合。计算机网络体系结构是抽象的,而实现是具体的,是能够运行的一些硬件和软件,多采用层次结构。划分层次的原则如下。

(1) 网中各节点都有相同的层次。

(2) 不同节点的同等层具有相同的功能。

(3) 同一节点内相邻层之间通过接口通信。

(4) 每一层使用下层提供的服务,并向其上层提供服务。

(5) 不同节点的同等层按照协议实现对等层之间的通信。

下面介绍各层的主要功能。

（1）物理层。这是整个OSI参考模型的最底层，它的任务就是提供网络的物理连接。所以，物理层是建立在物理介质上的（而不是逻辑上的协议和会话），它提供的是机械和电气接口，其作用是使原始的数据比特（bit）流能在物理媒体上传输。

（2）数据链路层。数据链路层分为介质访问控制（MAC）子层和逻辑链路控制（LLC）子层，在物理层提供比特流传输服务的基础上，传送以帧为单位的数据。数据链路层的主要作用是通过校验、确认和反馈重发等手段，将不可靠的物理链路改造成对网络层来说无差错的数据链路。数据链路层还要协调收发双方的数据传输速率，即进行流量控制，以防止接收方因来不及处理发送方来的高速数据而导致缓冲区溢出及线路阻塞等问题。

（3）网络层。网络层负责由一个站到另一个站间的路径选择，它解决的是网络与网络之间，即网际的通信问题，而不是同一网段内部的事。网络层的主要功能是提供路由，即选择到达目的主机的最佳路径，并沿该路径传送数据包（分组）。此外，网络层还具有流量控制和拥塞控制的能力。

（4）传输层。传输层负责提供两站之间数据的传送。当两个站已确定建立了联系后，传输层即负责监督，以确保数据能正确无误的传送，提供可靠的端到端数据传输。

（5）会话层。会话层主要负责控制每一站究竟什么时间可以传送与接收数据。例如，如果有许多使用者同时进行传送与接收消息，此时会话层的任务就要去决定是要接收消息或是传送消息，才不会有“碰撞”的情况发生。

（6）表示层。表示层负责将数据转换成使用者可以看得懂的有意义的内容，包括格式转换、数据加密与解密、数据压缩与恢复等功能。

（7）应用层。应用层负责网络中应用程序与网络操作系统间的联系，包括建立与结束使用者之间的联系，监督并管理相互连接起来的应用系统以及系统所用的各种资源。

数据在网络中传送时，在发送方和接收方有一个数据封装和解封装的过程，如图3-2所示。

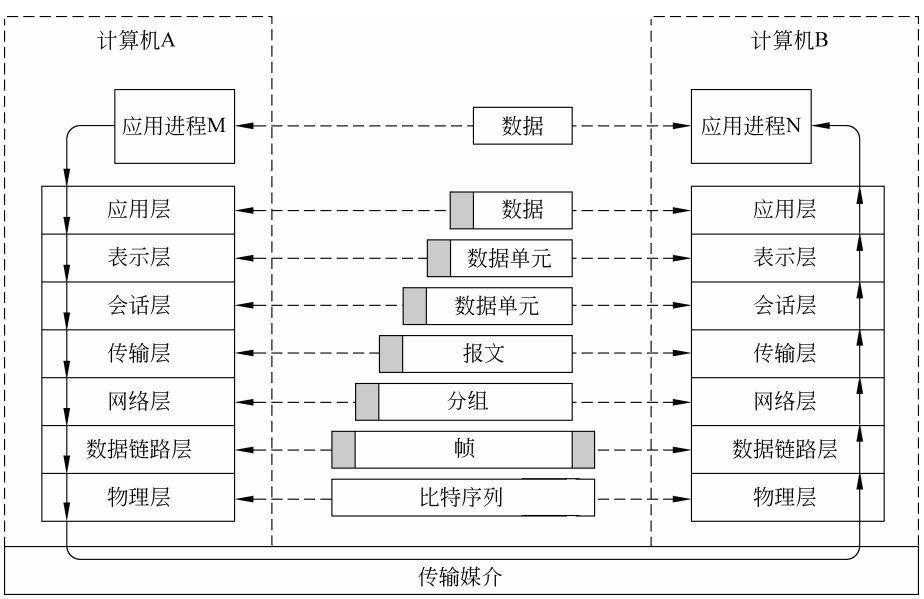

图3-2　数据的封装和解封装

(1) 当计算机 A 的应用进程 M 的数据传送到应用层时,应用层为数据加上本层控制报头后,组成应用层的服务数据单元,然后再传输给表示层。

(2) 表示层接收到这个数据单元后,加上本层的控制报头,组成表示层的服务数据单元,再传送给会话层,以此类推,数据被传送到传输层。

(3) 传输层接收到这个数据单元后,加上本层的控制报头,就构成了传输层的服务数据单元,它被称为报文(message)。

(4) 传输层的报文传送到网络层时,由于网络层数据单元的长度限制,传输层长报文将被分成多个较短的数据段(分片),加上网络层的控制报头,就构成了网络层的服务数据单元,它被称为分组(packet)。

(5) 网络层的分组传送到数据链路层时,加上数据链路层的控制信息(帧头和帧尾),就构成了数据链路层的服务数据单元,它被称为帧(frame)。

(6) 数据链路层的帧传送到物理层后,物理层将以比特(bit)流的方式通过传输媒介传输出去。当比特流到达目的节点计算机 B 时,再从物理层依层上传,每层对各层的控制报头进行处理后,将用户数据上交给上一层,最终将计算机 A 的进程 M 的数据传送给计算机 B 的进程 N。

尽管应用进程 M 的数据在 OSI 环境中经过复杂的处理过程才能送到另一台计算机的应用进程 N,但对于每台计算机的应用进程而言,OSI 环境中数据流的复杂处理过程是透明的。应用进程 M 的数据好像是“直接”传送给应用进程 N,这就是开放系统在网络通信过程中最本质的作用。

2. TCP/IP 参考模型

建立 OSI 体系结构的初衷是希望为网络通信提供一种统一的国际标准,然而其固有的复杂性等缺点制约了它的实际应用。一般而言,由于 OSI 体系结构具有概念清晰的优点,主要适用于教学研究。

ARPAnet 最初开发的网络协议使用在通信可靠性较差的通信子网中,且出现了不少问题,这就导致了新的网络协议 TCP/IP 的产生。虽然 TCP/IP 协议不是 OSI 标准,但它是目前最流行的商业化的网络协议,并被公认为是当前的工业标准或“事实上的标准”。

TCP/IP 协议具有以下特点。

(1) 开放的协议标准,独立于特定的计算机硬件和操作系统。

(2) 独立于特定的网络硬件,可以运行在局域网、广域网中,更适用于互联网。

(3) 统一的地址分配方案,使得整个 TCP/IP 设备在网中都具有唯一的地址。

(4) 标准化的高层协议,可提供多种可靠的服务。

TCP/IP 参考模型分为 4 层:网络接口层、网络层(互联层)、传输层和应用层。TCP/IP 参考模型与 OSI 参考模型的对应关系如表 3-1 所示。

TCP/IP 的网络接口层实现了 OSI 模型中物理层和数据链路层的功能。

TCP/IP 的网络层功能主要体现在以下三个方面:

(1) 处理来自传输层的分组发送请求;

(2) 处理接收的分组;

表 3-1　TCP/IP 参考模型与 OSI 参考模型的对应关系

OSI 参考模型	TCP/IP 参考模型	TCP/IP 常用协议
应用层	应用层	DNS、HTTP、SMTP、POP、Telnet、FTP、NFS
表示层		
会话层		
传输层	传输层	TCP、UDP
网络层	网络层	IP、ICMP、IGMP、ARP、RARP
数据链路层	网络接口层	Ethernet、ATM、FDDI、ISDN、TDMA
物理层		

（3）处理路径选择、流量控制与拥塞问题。

传输层实现应用进程间的端到端通信，主要包括两个协议：TCP 协议和 UDP 协议。

TCP 协议是一种可靠的面向连接的协议，允许将一台主机的字节流无差错地传送到目的主机。UDP 协议是不可靠的无连接协议，不要求分组顺序到达目的地。

应用层的主要协议有：域名系统（DNS）、超文本传输协议（HTTP）、简单邮件传输协议（SMTP）、邮局协议（POP）、远程登录协议（TELNET）、文件传输协议（FTP）、网络文件系统（NFS）等。

3.3.2　以太网的帧格式

1. MAC 地址

为了标识以太网上的每台主机，需要给每台主机上的网络适配器（网卡）分配一个全球唯一的通信地址，即 MAC 地址，或称为网卡的物理地址、Ethernet 地址。

IEEE 负责为网络适配器制造厂商分配 MAC 地址块，各厂商为自己生产的每块网络适配器分配一个全球唯一的 MAC 地址。MAC 地址长度为 48 比特，共 6 字节，如 00-0D-88-47-58-2C（十六进制），其中，前 3 字节为 IEEE 分配给厂商的厂商代码（00-0D-88），后 3 字节为厂商自己设置的网络适配器编号（47-58-2C）。MAC 广播地址为 FF-FF-FF-FF-FF-FF。如果 MAC 地址（二进制）的第 8 位是 1，则表示该 MAC 地址是组播地址，如 01-00-5E-37-55-4D。

2. 以太网的帧格式

以太网的帧是数据链路层的封装形式，网络层的数据包被加上帧头和帧尾成为可以被数据链路层识别的数据帧（成帧）。虽然帧头和帧尾所用的字节数是固定不变的，但依被封装的数据包大小的不同，以太网的帧长度也在变化，其范围是 64～1518 字节（不算 8 字节的前导字）。

以太网的帧格式有多种，在每种格式的帧开始处都有 64 比特（8 字节）的前导字符，其中前 7 字节为前同步码（7 个 10101010），第 8 字节为帧起始标志（10101011）。图 3-3 所示为 Ethernet Ⅱ的帧格式（未包括前导字符）。

Ethernet Ⅱ类型以太网帧的最小长度为 64 字节（6＋6＋2＋46＋4），最大长度为 1518 字节（6＋6＋2＋1500＋4）。其中前 12 字节分别标识出发送数据帧的源节点 MAC 地址和接收